

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Asst. Comm. for Patents, Washington, D.C. 20231, on this date.

March 14, 2001  
Date

L. Novila  
Express Mail Label No.: EL 846162085 US

APPLICATION FOR

UNITED STATES LETTERS PATENT

SPECIFICATION

INVENTOR(S): Takayoshi KURITA

Title of the Invention: SMART CARD ACCESS MANAGEMENT SYSTEM,  
SHARING METHOD, AND STORAGE MEDIUM

# SMART CARD ACCESS MANAGEMENT SYSTEM, SHARING METHOD, AND STORAGE MEDIUM

## Background of the Invention

### 5 Field of the Invention

The present invention relates to the access management of a smart card when the data on the smart card is shared by a plurality of processes.

### 10 Description of Related Art

Since a smart card can store a large volume of data as compared with a conventional magnetic card, it has been studied and put to practical use in various fields.

15 Furthermore, a smart card contains memory and a CPU to access data in the memory through the CPU. Therefore, the CPU performs an authenticating process when data is accessed, thereby realizing higher security than the conventional magnetic card.  
20 This advantageously marks a smart card.

A smart card has a security function of a PIN (personal identification number). That is, a matching check is performed on a PIN. Only if it is authenticated, the confidential information in a  
25 card can be accessed. The authentication system

using a PIN belongs to a password input system. A user of a smart card inputs, for example, a password as a PIN which is compared in the card with the password stored in the card. It they match  
5 each other, the user is permitted to access the data in the card.

A smart card can be accessed through a logical channel of the smart card, and an authentication request is issued to the logical channel. The smart  
10 card holds the status about the security such as an authentication status by a PIN, etc. for each logical channel.

FIG. 1 shows the logical configuration in a smart card from the viewpoint of an application.

15 In the smart card, data is managed in the configuration of a tree structure in which a DF (dedicated file) is provided by each an application unit, etc., below the highest-order DIR. Each DF stores an EF (elementary file) containing actual  
20 data. When data is accessed from a smart card, an application first transmits location information about the position of the data to be accessed, moves the access position to the target EF, and reads from or writes to the EF. In addition, each  
25 channel holds the current access position as status

information.

The method of using a smart card simultaneously by a plurality of applications has been studied. For example, when a PKI (public key infrastructure) system based on the public key encryption system is designed, and a plurality of applications are operated in a computer in the PKI system, a smart card can be used by an application in checking security using a digital signature, etc.

In this case, a plurality of applications in a computer to which the smart card is connected share the smart card. Since one smart card can have at most two logical channels, it is necessary for a plurality of applications to share one logical channel when the plurality of applications is permitted to access the same card. For simple explanation, the following descriptions in this specification are based on that one application is configured by one process, and a term 'application' is assumed to be synonymous with a 'process'. Normally, one application is configured by one process. However, although it is configured by a plurality of processes, the following descriptions are true with either case if an application is replaced with a process.

In the current smart card security system, if one application performs a PIN authentication process on a logical channel, and is permitted to access a card, then not only the authenticated application, but also other applications can access the card through the logical channel until the authentication is canceled.

From the viewpoint of security, sharing the same information on one card among a plurality of applications can be secured at a higher level when an authenticating process is performed using a PIN for each application. However, in controlling access to a smart card, an authenticating process is performed for each logical channel and an authentication status (whether or not permission to access a card is allowed) is held in each logical channel when a plurality of applications share one logical channel. Therefore, if one application obtains permission to access a card through an authentication process using a PIN, then another application can access the card through the logical channel without authentication by a PIN.

Furthermore, as described above, when each application accesses data in a card, it first transmits the location information to a logical

channel, moves the access position, and then writes  
or reads the data. However, when a plurality of  
applications share a logical channel, it is  
difficult to confirm the current access position  
5 for each application.

### Summary of the Invention

To solve the above mentioned problems, the  
present invention aims at providing a smart card  
10 access management system and method for allowing  
permission for each application (process) by  
centrally managing the authentication status of a  
smart card in response to access from a plurality  
of applications (processes). It also aims at  
15 providing an access management system and method  
for realizing authentication for each application  
(process) without increasing the overhead by an  
authenticating process.

The smart card access management system  
20 according to the present invention is based on the  
management of access to a smart card by a plurality  
of applications, and includes an exclusion control  
unit and an access control unit.

In response to an exclusive access request for  
25 a smart card from an application, the exclusion

control unit allows the application the exclusive access to the smart card if the smart card has a logical channel not exclusively accessed by another application. Furthermore, in response to an exclusive access request for a smart card from an application, the exclusion control unit queues the application requesting the exclusive access to the smart card if the smart card has no logical channel which is not exclusively accessed by another application.

In response to an access request for the smart card from an application allowed the exclusive access, the access control unit permits the application allowed the exclusive access to access the smart card when the application allowed the exclusive access has already been authenticated for the smart card. In response to the access request, the access control unit requests the application to input a PIN when the application allowed the exclusive access has not been authenticated for the smart card. A smart card is authenticated for each application through the access control unit, and the access control unit grasps the authentication between each application and the smart card.

According to the present invention, since the

exclusion control unit controls the exclusive access to a smart card, an authenticating process can be performed for each application although a plurality of applications share a smart card.

5           Furthermore, since the access control unit determines whether or not an application issuing each access request has been authenticated, permission to access a card is allowed without performing an authenticating process if it has  
10           already been authenticated, thereby reducing the times of authenticating processes.

#### **Brief Description of the Drawings**

15           FIG. 1 shows the logical configuration inside a smart card;

            FIG. 2 shows the configuration when an exclusion control mechanism is provided to allow exclusive access to a smart card;

20           FIG. 3 shows a process of each application accessing a smart card when an exclusion control mechanism is provided;

            FIG. 4 shows the configuration provided with an exclusion control mechanism and an access control mechanism;

25           FIG. 5 shows an example of the configuration



of an authentication status management table;

FIG. 6 is a flowchart of the process of an application, an exclusion control mechanism, and an access control mechanism when an application  
5 accesses a smart card;

FIG. 7 shows a process of each application accessing a smart card when an exclusion control mechanism and an access control mechanism are provided;

10 FIG. 8 is a flowchart of the process of an application accessing a smart card;

FIG. 9 is a flowchart of the process of an exclusion control mechanism in response to an exclusive access request from an application;

15 FIG. 10 is a flowchart of the process of an exclusion control mechanism in response to an exclusion cancellation notification from an application;

FIG. 11 is a flowchart of the process of an access control mechanism in response to an access start declaration from an application to a smart  
20 card;

FIG. 12 is a flowchart of the process of an access control mechanism in response to an access  
25 request from an application to a smart card;

FIG. 13 shows the configuration of the system using a smart card according to an embodiment of the present invention;

FIG. 14 shows a system environment of an information processing device; and

FIG. 15 shows an example of a storage medium.

#### Description of the Preferred Embodiment

A preferred embodiment of the present invention is described below by referring to the attached drawings.

To authenticate each application, it is necessary to allow exclusive access to a smart card (a logical channel when a smart card has a plurality of logical channels), the application occupies the card (or the logical channel) while an authenticated application is using the smart card, and access from other applications has to be suppressed. For simple explanation, it is assumed in the embodiment below that each smart card is assigned one logical channel. When a smart card is provided with a plurality of logical channels, the exclusion control described below is performed in a logical channel unit.

FIG. 2 shows the case in which an exclusion

control mechanism is provided to allow an application exclusive access to a smart card.

In FIG. 2, an exclusion control mechanism 11 is provided between a plurality of applications 21 and a smart card 22, each application 21 issues an exclusive access request to the exclusion control mechanism 11 when it requests to access the smart card 22, and an application 21 which has successfully been allowed exclusive access can exclusively access the smart card 22. The exclusion control mechanism 11 shown in FIG. 2 manages the exclusive access to two cards, that is, a card a and a card b. Three applications 21, that is, an AP 1, an AP 2, and an AP 3, issue requests to access the card a, and the exclusion control mechanism 11 allows the AP 1 exclusive access, and keeps other APs 2 and 3 waiting until the card a is released. The AP 1 allowed the exclusive access reads/writes data after authenticating the logical channel of the card a using a PIN. On the other hand, other applications 21 cannot access the card a. When the AP 1 releases the card A after completing the process, then the waiting AP 2 obtains exclusive access, authenticates the card a using a PIN, and accesses the data inside. Thus, by providing the

exclusion control mechanism 11, only one application can access a smart card, and the authenticating process can be performed on each application 21.

5           In the system with the configuration shown in  
FIG. 2, the smart card 22 is occupied by one  
application 21 while the application 21 is using  
the smart card 22. Therefore, other applications 21  
enters a wait state until the exclusive access of  
10   the application 21 is canceled and the smart card  
22 is released. As a result, in this system, a  
plurality of applications cannot efficiently  
perform parallel processes. And the applications in  
the wait state seem to be hung-up, because the  
15   applications have to stop their processes for a  
long time, so this system may not be so easy to  
handle.

          To avoid this inconvenience, the application  
21 can sequentially release the occupied smart card  
20   22 upon completion of the accessing process on the  
smart card 22. In this system, when the application  
21 performs plural times the accessing process on  
the smart card 22, the application 21 requests the  
exclusion control mechanism 11 for exclusive access  
25   to the smart card 22 and release of it, that is,

the exclusive access is delimited in pieces.

FIG. 3 shows an example of the exclusive access to and release of a smart card by each application.

5           FIG. 3 shows an example of the process of the three applications 21, that is, the APs 1, 2, and 3 as in the case shown in FIG. 2, accessing a smart card when they issue requests to access the card a. In FIG. 3, the arrow  $\uparrow$  to the exclusion control mechanism 11 indicates a request from each application 21 to the exclusion control mechanism 11 to obtain exclusive access, and the arrow  $\downarrow$  from the exclusion control mechanism 11 indicates an exclusive access notification from the exclusion control mechanism 11 to each application 21. The hatched portion indicates an authenticating process using a PIN, and a net portion indicates the process of accessing the smart card 22.

10

15

If the application 21 allowed exclusive access does not cancel the exclusive access and release the smart card 22 until the entire process is completed, the AP 2 is set in the wait state from the position 31 shown in FIG. 3 at which the AP 2 issued the exclusive access request to the exclusion control mechanism 11 to the position 33

20

25

at which the AP 1 already allowed the exclusive access to the card a completes the process. The AP 3 is also set in the wait state from the position 32 to the position at which the AP 2 completes the process. However, if the application 21 shown in FIG. 3 delimits the exclusive access in pieces for each accessing process, another application 21 can access the card a while the exclusive access is being canceled, thereby shortening the waiting time in which applications are kept waiting by the exclusive access, and improving the parallelism of the processes.

Thus, by frequently switching the exclusion control, the waiting time of each application can be shortened and the parallelism of the processes can be improved. However, as shown by the hatched portion shown in FIG. 3, it is necessary that each application has to set and release the authentication status each time control is switched, thereby increasing overhead. Furthermore, since a PIN is transmitted to request again authentication permission, each application 21 continues holding the PIN, thereby causing the problem with security. If a user inputs a password in each authenticating process to avoid this problem, the authenticating

process furthermore increases the overhead.

FIG. 4 shows the configuration with the above mentioned problem taken into account.

In the configuration shown in FIG. 4, an  
5 access control mechanism 12 is provided in addition  
to the exclusion control mechanism 11 between the  
application 21 and the smart card 22. While the  
access control mechanism 12 is centrally managing  
the authentication of each application 21 for the  
10 smart card 22, the exclusion control mechanism 11  
allows the application 21 exclusive access to the  
smart card 22.

When each application 21 requests access to  
the smart card 22, it first requests the exclusion  
15 control mechanism 11 to allow the application 21  
exclusive access, and then requests the access  
control mechanism 12 to authenticate the smart card  
22 when it is allowed the exclusive access. When  
the authenticating process is successfully  
20 performed, the application accesses the data in the  
smart card 22.

The access control mechanism 12 has an  
authentication status management table. Using the  
authentication status management table, the access  
25 control mechanism 12 manages the authentication

status between each application and the smart card 22 after the application 21 declares the start of authentication of the smart card 22 until it issues an authentication release notification.

5           FIG. 5 shows an example of the configuration of the authentication status management table.

10           The authentication status management table is used by the exclusion control mechanism 11 managing the current authentication state of each application 21 for the smart card 22, and stores application identification information associated with authenticated card information. The application identification information stores unique identifier for identification of each application 21. The identifier cannot be operated by a common application. For example, it can be a process ID which is managed by a kernel, and is assigned to each process when the process is generated. Otherwise, an identifier can be sequentially generated by the access control mechanism 12 for the application 21 which requests access to a smart card.

15           

20           

25           FIG. 5 shows an example of an authentication status management table when the authentication status of each application 21 for the two smart



cards 22, that is, the cards a and b. The authentication status management table stores the cards for which the application 21 is authenticated as the authenticated card information for each application. The blank portion for the authenticated card information indicates that there are no smart cards authenticated for the application. In FIG. 5, the AP 1 has been authenticated for the cards a and b, but the APs 2 and n have not been authenticated for any card, and the AP 3 has been authenticated only for the card a.

Each application 21 is authenticated for the smart card 22, and accesses the smart card 22 through the access control mechanism 12. When the application 21 issues an access request to the smart card 22, the access control mechanism 12 checks by referring to the authentication status management table whether or not the application 21 has already been authenticated for the smart card 22 to which the application 21 requests to access. If it has not been authenticated yet, the access control mechanism 12 rejects the request from the application 21, and requests the application 21 to input a PIN to perform an authenticating process for the smart card 22. If the application 21 has

already been authenticated, the application 21,  
 then the application 21 has already allowed the  
 authentication permission for the application 21,  
 and the access to the application 21 is permitted  
 5 and executed.

FIG. 6 is a flowchart of the process of the  
 application 21, the exclusion control mechanism 11,  
 and the access control mechanism 12 when the  
 application 21 accesses the smart card 22. FIG. 6  
 10 shows an example of the AP 1 accessing the card a,  
 and 1) through 23) in the descriptions correspond  
 to the numbers shown in FIG. 6.

1) The AP 1 requests the exclusion control  
 mechanism 11 to allow exclusive access to the card  
 15 a to start the exclusive access.

2) Upon receipt of the request from the AP 1, the  
 exclusion control mechanism 11 checks whether or  
 not there is an application allowed exclusive  
 access to the card a. If another application has  
 20 already been allowed the exclusive access to the  
 card a, then the AP 1 is queued for exclusive  
 access. If no applications have been allowed the  
 exclusive access to the card a, the AP 1 receives  
 an exclusive access notification.

25 3) The AP 1 declares the start of accessing the

card a on the access control mechanism 12.

4) In response to the access start declaration, the access control mechanism 12 registers the AP 1 in the authentication status management table. Then,  
5 it requests the AP 1 to input a PIN. If the AP 1 has also declared the start of accessing the card b, the AP has already been registered in the authentication status management table. Therefore, it is not necessary to register it again in the  
10 authentication status management table by declaring the start of accessing the card a.

5) The AP 1 prompts the user to input a password, specifies a PIN from the input of the user, and requests the authentication for the card a.

15 6) The exclusion control mechanism 11 notifies the card a of the PIN, and has the card a make an authentication check.

7) The access control mechanism 12 registers in the authentication status management table that the  
20 AP 1 has been authenticated for the card a if the authentication check made by the card a indicates successful authentication.

8) The AP 1 requests the access control mechanism 12 to read or write data from or to the card a.

25 9) Upon receipt of the read/write request from

the AP 1, the authentication status management table is searched. If the AP 1 has been authenticated for the authenticated card a, then the AP 1 accesses the card a. If the AP 1 has not  
 5 been authenticated for the authenticated card a, then the AP 1 is notified of an error.

10) When one accessing process is completed and the card a is released, the AP 1 notifies the exclusion control mechanism 11 of the cancellation  
 10 of the exclusive access.

11) The exclusion control mechanism 11 deletes the registered exclusive access to the card a by the AP 1, and registers the exclusive access of another application 21 if it is registered in the queue  
 15 waiting for exclusive access to the card a.

12) After canceling the exclusive access, the AP 1 performs a process other than the accessing process to the card a. During the period, the card a is released from the exclusive access. Therefore,  
 20 another application 21 can use the card a.

13) The AP 1 requests the exclusion control mechanism 11 to allow the AP 1 exclusive access when it is necessary again to access the card a.

14) In response to the request from the AP 1, the  
 25 exclusion control mechanism 11 checks again whether

or not there is exclusive access to the card a as in the case 2) above. If another application has not been allowed exclusive access, the AP 1 is notified of the exclusive access.

5 15) The AP 1 requests the access control mechanism 12 to read/write data to the card a.

16) The access control mechanism 12 performs the process of 9) above. At this time, since it is registered in the authentication status management  
10 table that the AP 1 has been authenticated for the card a in 7) above, the AP 1 accesses the card a as is. Then, the processes of 10) through 16) are repeated the number of times of the accessing process to the card A in the AP 1.

15 17) When all accessing processes are completed, the AP 1 notifies the access control mechanism 12 of the cancellation of the authentication for the card a.

18) The access control mechanism 12 deletes the  
20 information about the authentication of the AP 1 for the card a in the authentication status management table.

19) The access control mechanism 12 holds the authentication status until no application  
25 authenticated for the card a can be detected in an

authentication status management table 13. When no application 21 authenticated for the card a can be detected in the table, the access control mechanism 12 requests the card a to cancel the authentication.

5 Thus, times of the accessing process for the same smart card can be reduced.

20) The AP 1 notifies the access control mechanism 12 of the completion of the access to the smart card 22.

10 21) Upon receipt of the notification in 20) above, the access control mechanism 12 deletes the AP 1 from the authentication status management table. At this time, if the AP 1 has not completed the access to another smart card 22, then the AP 1 is not  
15 deleted from the authentication status management table.

22) The AP 1 notifies the exclusion control mechanism 11 of the cancellation of the exclusive access to the card a.

20 23) The exclusion control mechanism 11 performs the process similar to the process in 11) above, and the exclusive access is canceled.

FIG. 7 shows the process performed by each application on a smart card with the configuration  
25 containing the exclusion control mechanism 11 and

the access control mechanism 12 shown in FIG. 4.

FIG. 7 shows the process of the same application 21 based on the same conditions shown in FIG. 3 for correct comparison. In FIG. 7, as compared with FIG. 3, each application 21 performs the authenticating process using a PIN when the accessing process to the first card a is started, and the authentication canceling process for the card a when the last accessing process is completed. However, the authenticating process performed as shown in FIG. 3 for each accessing process to the card a is omitted. Therefore, the processing time required for each application 21 can be shortened by the time required for the omitted authenticating process. Since the period of each application 21 occupying the card a can also be shortened by the period of the omitted authenticating process, there is some possibility of shortening a period of the wait state. Furthermore, since each application 21 has to once perform an authenticating process using a PIN for the smart card 22, the application 21 can discard the PIN after obtaining authentication from the card.

FIG. 8 is a flowchart of the process of the application 21 accessing the smart card 22

according to the present system.

The mechanism for performing the following processes can be configured in the application 21. However, the processes can normally be realized as  
 5 a library, and the library can be incorporated into each application 21.

When the application 21 accesses the smart card 22, it first requests the exclusion control mechanism 11 to allow it exclusive access to the  
 10 card (step S1), and waits for the response from the exclusion control mechanism 11. As a result, when the exclusion control mechanism 11 notifies the application 21 that the exclusive access cannot be allowed for any reason (NO in step S2), the process  
 15 terminates.

If the exclusion control mechanism 11 notifies the application 21 of a successful exclusive access notification in response to the exclusive access request (YES in step S2), then in step S3 a  
 20 declaration of the start of the access to the smart card 22 is issued to the access control mechanism 12.

If the smart card 22 to which access is gained is not authenticated, and if the access control  
 25 mechanism 12 prompts the application to input a PIN



to obtain authentication for the smart card 22 (YES in step S4), then the password inputted by the user as the PIN is transmitted to the access control mechanism 12 for an authenticating process. Then, the result is confirmed. If the authentication can be successfully obtained (YES in step S9), then control is passed to step S5, and the smart card is accessed. If the authentication cannot be successfully obtained (NO in step S9), then the process terminates.

When access is gained to the smart card 22 which has already been authenticated in step S4 (NO in step S4), a further authenticating process is not required. Therefore, access to the smart card 22 is allowed in step S5 to read/write data.

When the accessing process in step S5 is completed, a declaration of the completion of the access to the smart card 22 is issued to the access control mechanism 12 in step S6. Then, in step S7, the exclusion control mechanism 11 is notified of the cancellation of the exclusive access to the smart card 22, and the process of accessing the smart card 22 terminates.

FIG. 9 is a flowchart of the process of the exclusion control mechanism 11 in response to the

exclusive access request from the application 21.

Upon receipt of an exclusive access request to the smart card 22 from the application 21, the exclusion control mechanism 11 determines in step S11 whether or not the smart card 22 for which the exclusive access request has been issued has already been exclusively accessed by another application 21. As a result, if the smart card 22 has not been exclusively accessed by another application 21 (NO in step S11), it is registered that the smart card 22 has already been exclusively accessed, the requesting smart card 22 is notified of the exclusive access, and the process terminates.

If another application 21 has already been allowed exclusive access to the smart card 22 in step S11 (YES in step S11), then the exclusive access request is queued in step S12, and the process terminates.

FIG. 10 is a flowchart of the process of the exclusion control mechanism 11 performed in response to an exclusive access cancellation notification from the application 21.

Upon receipt of the notification about the cancellation of exclusive access to the smart card 22 from the application 21, the exclusion control

mechanism 11 deletes the registration that the application 21 has been allowed exclusive access in step S21, and then the exclusive access is canceled.

Then, the exclusive access waiting queue is  
 5 checked. If there is any application 21 waiting for exclusive access to the smart card 22 for which exclusive access has been canceled (YES in step S22), then the exclusive access to the smart card 22 from the application 21 which is registered as  
 10 the first application in the exclusive access waiting queue is registered, and the smart card 22 is dispatched in step 23, and the process terminates. At this time, if no application is in the exclusive access waiting queue (NO in step S22),  
 15 the process terminates.

FIG. 11 is a flowchart of the process of the access control mechanism 12 performed in response to an access request from the application 21 to the smart card 22.

20 In response to the declaration of the start of the access from the application 21, the access control mechanism 12 registers the application 21 in the authentication status management table, and registers an access request process for the smart  
 25 card 22 in step S31.

FIG. 12 is a flowchart of the process of the access control mechanism 12 performed in response to the access request from the application 21 to the smart card 22.

5           In response to the access request from the application 21, the access control mechanism 12 refers to the authentication status management table in step S41, and checks whether or not the application 21 has already been authenticated for the smart card 22 for which the application 21 has  
10           issued the access request. As a result, if it has already been authenticated (YES in step S41), no further authentication is required, thereby notifying the application 21 of the access  
15           permission in step S45.

          If the application 21 has not been authenticated in step S41 (NO in step S41), then it is necessary to perform an authenticating process. Therefore, in step S42, the application 21 is  
20           prompted to input a password, and it is requested that the authenticating process is performed for the smart card 22 using a PIN. If the authentication for the smart card 22 can be  
25           obtained, then the application 21 is allowed access in step S45. If the authentication cannot be

allowed (NO in step S43), then the application 21 is notified of an access rejection notification, thereby terminating the process.

FIG. 13 shows the configuration of the system using a smart card according to the present embodiment.

An access management system 40 for management between an application 41 and a smart card 42 according to the present embodiment is provided between a smart card leader 43 and a library 44 of each application 41, and is realized as the installation as a function of an OS or in the OS.

The application 41 performs the authenticating process and an accessing process on the smart card 42 through the access management system 40. The access management system 40 grasps the transmission and reception of data between each application 41 and the smart card 42. Furthermore, the access management system 40 grasps the status of the smart card leader 43. For example, when the smart card 42 is extracted from the smart card leader 43, the authentication status management table is checked. If there is any application already authenticated for the card, it is changed as being non-authenticated.

Although the access management system 40 is configured as having the exclusion control mechanism 11 and the access control mechanism 12 separately inside the system, they can be realized as one function component. Additionally, for increased security, it is necessary that an access control mechanism and an exclusion control mechanism can be shared by a plurality of applications. Therefore, if they are realized in the kernel of an OS, the security can be furthermore improved.

FIG. 14 shows the system environment of the information processing device when the above mentioned smart card access management according to an embodiment of the present invention is realized by a computer program.

An information processing device using a smart card comprises, as shown in FIG. 14, a CPU 51, a main storage device 52 including ROM and RAM, an auxiliary storage device 53, an input/output device (I/O) 54 such as a display, a keyboard, etc., a LAN, a WAN, a network connection device 55 such as a modem, etc. for network connection to another information processing device through a common line, etc., a medium read device 56 for reading stored

contents from a portable storage medium 57 such as a disk, a magnetic tape, etc., and a smart card leader 58 containing one or more smart cards 59. These components are connected through a bus 60.

5           In the information processing system shown in FIG. 14, the medium read device 56 reads a program and data stored in the portable storage medium 57 such as a magnetic tape, a floppy disk, CD-ROM, MO, etc., and downloads them onto the main storage  
10 device 52 or the hard disk 55. Each process according to the present embodiment can be realized as software by the CPU 51 executing the program and the data.

          In this information processing device,  
15 application software can be exchanged using the portable storage medium 57 such as a floppy disk, etc. Therefore, the present invention is not limited to the smart card access management system or sharing method, but can be configured as a  
20 computer-readable storage medium 57 used to direct a computer to perform the function according to the embodiment of the present invention.

          In this case, a storage medium can be, for example, as shown in FIG. 15, a portable storage  
25 medium 76 removable from a medium drive device 77

such as CD-ROM, a floppy disk (or MO, DVD, a removable hard disk, etc.), etc., a storage unit (database, etc.) 72 in an external device (server, etc.) transmitted through a network line 73, memory  
5 (RAM or a hard disk, etc.) 75, etc. in a body 74 of an information processing device 71. A program stored in the portable storage medium 76 and the storage unit (database, etc.) 72 is loaded onto the memory (RAM, hard disk, etc.) 75 in the body 74,  
10 and executed.

As described above, according to the present invention, since the exclusion control is performed on a smart card by an exclusion control mechanism, each application is authenticated although a  
15 plurality of applications share a smart card.

In addition, since the authentication between each application and a smart card is centrally managed, it is determined whether or not an application has been authenticated for a smart card  
20 when the application issues a request to access the smart card, and an authenticating process is performed only when it has not been authenticated, thereby reducing the times of the authenticating processes, and also reducing the overhead from the  
25 authenticating process. In addition, since the



authenticating process using a PIN is once performed at first, it is not necessary for an application to keep holding a PIN, and the security level can be enhanced.

- 5           Furthermore, a smart card can be accessed among a plurality of authenticated applications with the authentication status held as is.

- 10           In addition, the waiting period of an application for exclusive access can be shortened. Therefore, the parallelism of processes can be improved, and the processing time of each application can be shortened.

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208